

WHAT IS CLAIMED IS:

1. A storing apparatus for protecting an access of information recorded on a medium by a password, comprising:

5 a password preserving unit for preserving a
default input password and a password for access
protection; and

a password verifying unit for controlling the access protection by substituting said default input password for a user input password and comparison collating with said password for access protection when there is no password input from the user and for controlling the access protection by comparison collating the user input password with said password for access protection when there is the password input from the user.

2. An apparatus according to claim 1, wherein in the case where a same value has been preserved in said default input password and said password for access protection by said password preserving unit, even if there is no password input by the user, said password verifying unit permits an access by substituting said default input password for the user input password and collating with the password for access protection.

3. An apparatus according to claim 1, wherein

said password preserving unit further has a user input password area to store the user input password, and

5 said password verifying unit is constructed in a manner such that

10 at the start of the use of the apparatus such as turn-on of a power source, command reset, error reset, further, medium insertion, or the like, said default input password is read out and written into said user input password area, an access permission or inhibition is subsequently established on the basis of a collation coincidence between the password in said user input password area and said password for access protection,

15 after the access permission was established, each time there is a password input of the user, the user input password is written into said user input password area and, subsequently, the access permission or inhibition is established on the basis of a collation coincidence between the password in said user input password area and said password for access protection.

25 4. An apparatus according to claim 1, wherein said password preserving unit further has a user input password area to store the user input password, and

 said password verifying unit is constructed in a manner such that

at the start of the use of the apparatus such as
turn-on of a power source, command reset, error reset,
further, medium insertion, or the like, the apparatus
waits for the password input by the user in a state
5 where said default input password is read out and
written into said user input password area,

when there is the user password input, the user
input password is overwritten into the default input
password in said user input password area, and after
10 that, the password in said user input password area and
said password for access protection are collated and
compared and the access protection is controlled, and

when there is no user password input and/or in the
case where the password is an empty character train
15 even if there is the user password input, the collation
comparison between the default input password in said
user input password area and said password for access
protection is executed and the access protection is
controlled.

20 5. An apparatus according to claim 1, wherein said
password preserving unit preserves said default input
password and said password for access protection into a
non-volatile memory of an apparatus main body.

25 6. An apparatus according to claim 1, wherein
said password preserving unit preserves said

default input password and said password for access protection into said medium, and

5 said password verifying unit reads out said default input password and said password for access protection from said medium and stores into an apparatus main body at the start of the use of the apparatus and controls the access protection.

10 7. An apparatus according to claim 1, wherein said password preserving unit preserves said default input password into a non-volatile memory of an apparatus main body and preserves said password for access protection into the medium, and

15 said password verifying unit reads out said password for access protection from said medium and stores into the apparatus main body at the start of the use of the apparatus and controls the access protection.

20 8. An apparatus according to claim 1, wherein said password verifying unit preserves said password for access protection into a non-volatile memory of an apparatus main body and preserves said default input password into the medium, and

25 a password processing unit reads out said default input password from said medium and stores into the apparatus main body at the start of the use of the

apparatus and controls the access protection.

9. An apparatus according to any one of claims 5 to 7, wherein in said medium, a password preserving area to preserve said password is provided in a specific area which cannot be accessed by ordinary read command and write command.

10. An apparatus according to claim 1, further comprising a password rewriting unit for rewriting said default input password or said password for access protection on the basis of a dedicated command from an upper apparatus.

11. An apparatus according to any one of claims 5 to 7, wherein said medium is a medium fixedly enclosed in the apparatus main body.

12. An apparatus according to any one of claims 5 to 7, wherein said medium is a removable medium which is detachable for the apparatus main body.

13. An apparatus according to claim 1, wherein said password preserving unit preserves a plurality of kinds of passwords for access protection according to kinds of access protection, and said password verifying unit permits an access by

an ordinary command corresponding to the kind of said password for access protection in which a collation coincidence is obtained.

- 54
14. An apparatus according to claim 13, wherein
as said passwords for access protection, said password preserving unit preserves a write/read password to permit an access by a read command and a write command and a read only password to permit only
10 an access by the read command, and
said password verifying unit permits the access by the ordinary write command or read command when the collation coincidence of said write/read password is obtained and permits the access by only the ordinary
15 read command when the collation coincidence of said read only password is obtained.

- Sub
15
20 15. An apparatus according to claim 1, further comprising a validity term setting unit for setting a validity term into said default input password.

16. An apparatus according to claim 15, wherein said validity term setting unit counts the number of using times of the apparatus by a counter and, when a value
25 of said counter reaches a predetermined value, said validity term setting unit forcibly changes said default input password to a value different from the

default password so far.

17. An apparatus according to claim 15, wherein said validity term setting unit sets a time of a validity term and, when a present time in case of using the apparatus exceeds said validity term, said validity term setting unit forcibly changes said default input password to a value different from the default password so far.

18. A storing method of protecting information recorded on a medium from an access by a password, comprising:

a password preserving step of preserving a default input password and a password for access protection; and

a password verifying step of controlling the access protection by substituting said default input password for a user input password and comparison collating with said password for access protection when there is no password input from the user and for controlling the access protection by comparison collating said user input password with said password for access protection when there is the password input from the user.

19. A method according to claim 18, wherein in the

case where a same value has been preserved in said default input password and said password for access protection, in said password verifying step, prior to the password input of the user, a value of said default
5 input password is copied to the user input password and is collated with said password for access protection, thereby permitting or inhibiting an access.

~~Sub 7C~~ 20. A method according to claim 18, wherein
10 in said password preserving step, a plurality of kinds of passwords for access protection according to kinds of said access protection are preserved, and
in said password verifying step, an access by an ordinary command corresponding to the kind of said
15 password for access protection in which a collation coincidence is obtained is permitted.

~~Sub 7D~~ 21. A method according to claim 18, further comprising
20 a validity term setting step of setting a validity term into said default input password.